UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/936,132	09/04/2001	Liqun Chen	B-4294PCT 619054-4	9457

22879 7590 02/24/2005

HEWLETT PACKARD COMPANY
P O BOX 272400, 3404 E. HARMONY ROAD
INTELLECTUAL PROPERTY ADMINISTRATION
FORT COLLINS, CO 80527-2400

EXAMINER	
NOBAHAR, ABDULHAKIM	
ART UNIT	**PAPER NUMBER**
2132	

DATE MAILED: 02/24/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/936,132	CHEN ET AL.	
	Examiner	Art Unit	
	Abdulhakim Nobahar	2132	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☐ Responsive to communication(s) filed on _____.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-19 and 22-29* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-5,8-19,22,23 and 26-29* is/are rejected.

7)☒ Claim(s) *6,7,24 and 25* is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date *11/28/03,3/3/03*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

Claim Objections

Claims 1, 3-9 are objected to because of the following informalities: misspelling.

Regarding claims 1, 3-9, 15, 17, 18 and 19, the word "authorised" should be spelled as "authorized'.

Appropriate correction is required.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

1. Claims 1, 3-5, 8, 9, 13-15, 17-19, 22 and 29 are rejected under 35 U.S.C. 103(a) as being unpatentable over Handelman et al (6,298,441 B1; hereinafter Handelman) in view of Holtey (5,442,704).

Regarding claim 1, Handelman discloses a computing apparatus comprising:

memory means storing the instructions of a secure process and an authentication process (col. 5, lines 52-67; col. 7, lines 47-60; col. 9, lines 12-21; col. 11, lines 5-46);

processing means arranged to control the operation of the computing apparatus including by executing the secure process and the authentication process (col. 5, lines 52-67; col. 7, lines 47-60; col. 9, lines 12-21; col. 11, lines 5-46);

user interface means arranged to receive user input and return to the user information generated by the processing means in response to the user input (col. 11, lines 5-46); and

interface means for receiving a removable primary token and communicating with the token, the token comprising a body supporting (col. 8, lines 49-60):

a token interface for communicating with the interface means (col. 3, lines 30-48; Fig. 4; Fig. 7);

a token processor (col. 14, lines 21-28), and

token memory storing token data including information for identifying the token and auxiliary token information identifying one or more authorized auxiliary tokens (col. 4, line 38-col. 5, line5; col. 8, lines 10-18; col. 15, lines 34-50, where the main card also retains billing information of the restricted programs viewable only by using the parent card that corresponds to the auxiliary card),

wherein the processing means is arranged to receive the identity information and the auxiliary token information from the primary token (Fig. 3, CPU 62; col. 8, lines 10-18, where the main card also retains billing information of the restricted programs viewable only by using the parent card that corresponds to the auxiliary card), authenticate the token using the authentication process and, if the token is successfully

authenticated, permit a user to interact with the secure process via the user interface means (col. 5, line 65-col. 6, lines 6; col. 7, lines 47-56; col. 14, lines 58-66),

and cause the computing platform to suspend interaction between the secure process and the user if authentication is not possible as a result of the removal of the primary token unless the primary token is replaced by an authorized auxiliary token (col. 8, lines 19-60; col. 11, lines 32-46, where the absence of smart card corresponds to the recited the removal of the primary token; col. 12, lines 27-29; Fig. 8, where leaving the program scrambled corresponds to the recited to suspend interaction).

However, Handelman does not expressly disclose that the processing means is arranged to repeatedly authenticate the primary token.

Holtey discloses an access control system using smart cards that re-authenticate the system user (corresponding to the recited repeatedly authenticate the primary token) at an adjustable time interval (col. 6, lines 60-col. 7, lines 8).

Therefore, it would have been obvious to a person of ordinary skill in the art at the time the invention was made to implement a periodic authentication (i.e., repeated authentication) measure as taught in Holtey in the system of Handelman because it would provide a mechanism to enforce security (Holtey, col. 7, lines 5-8).

Regarding claim 3, Handelman discloses a smart or IC card that includes all forms of cards that are used for different application such as a smart card for purchasing a service or a document according to a spending limit that corresponds to the recited to credit or debit the token (col. 2, line 55-col. 3, line14).

Regarding claim 4, Handelman discloses: the authorized token is a crypto token programmed to encrypt, decrypt or sign data, and the secure process is arranged to transmit data to the crypto token to be encrypted, decrypted or signed and receive encrypted, decrypted or signed data from the crypto token (col. 3, lines 20-27; col. 11, lines 5-15; col. 18, lines 41-47).

Regarding claim 5, Handelman discloses: computing apparatus according to claim 1, arranged, only if the different token is an authorized auxiliary token, to allow the user to interact with the secure process (col. 5, lines 1-27).

Regarding claims 8 and 9, Handelman discloses: computing apparatus according to claim 1, arranged to permit interaction between the secure process and one or more authorized auxiliary token after removal of the primary token (col. 3, lines 40-47; col. 8, lines 7-9, where the parent card corresponds to the recited primary token).

Regarding claim 13, Handelman discloses: computing apparatus according to claim 1, wherein the primary token comprises a smart card (col. 2, lines 55-59), and the interface means is configured to receive a smart card (col. 8, lines 49-60).

Regarding claim 14, Handelman discloses: computing apparatus according to claim 1, wherein the auxiliary token information is stored in a user profile (col. 8, lines 10-18; col. 13, lines 46-54; col. 15, lines 34-50, where the authorization information read

from the card 400 corresponding to the recited auxiliary token are sent to the remote device 355 for authentication purpose. Thus, the user authorization information must exist at the remote device, with the other user information corresponding to the user profile).

Regarding claim 15, Handelman discloses: A method of controlling computing apparatus to authenticate a user, comprising the steps:

the computing apparatus receiving a primary token of the user, the primary token containing information suitable for authenticating the primary token and information relating to one or more authorized auxiliary tokens (col. 4, line 38-col. 5, line5; col. 8, lines 10-18; col. 15, lines 34-50, where the main card also retains billing information of the restricted programs viewable only by using the parent card that corresponds to the auxiliary card);

if the token is authentic, permitting the user to interact with one or more secure applications that may be executed by the computing platform (col. 5, line 65-col. 6, lines 6; col. 7, lines 47-56; col. 15, lines 34-50); and

if it is not possible to authenticate the primary token, suspending the interaction between the computing apparatus and the user unless the primary token has been replaced with an authorized auxiliary token (col. 8, lines 19-60; col. 11, lines 32-46, where the absence of smart card corresponds to the recited the removal of the primary token; col. 12, lines 27-29; Fig. 8, where leaving the program scrambled corresponds to the recited to suspend interaction).

However, Handelman does not expressly disclose that at intervals, re-authenticating the primary token.

Holtey discloses an access control system using smart cards that re-authenticate the system user (corresponding to the recited repeatedly authenticate the primary token) at an adjustable time interval (col. 6, lines 60-col. 7, lines 8).

Therefore, it would have been obvious to a person of ordinary skill in the art at the time the invention was made to implement a periodic authentication (i.e., repeated authentication) measure as taught in Holtey in the system of Handelman because it would provide a mechanism to enforce security (Holtey, col. 7, lines 5-8).

Regarding claim 17, Handelman discloses: A method according to claim 15, wherein the computing apparatus interaction with the authorized auxiliary token for a limited period of time (col. 3, lines 10-14, where the interaction is limited to the spending amount).

Regarding claims 18 and 19, Handelman discloses: A method according to claim 15, wherein the computing apparatus permits interaction with one or plural authorized auxiliary token after removal of the primary token (col. 3, lines 40-47; col. 8, lines 7-9, where the parent card corresponds to the recited primary token).

Regarding claim 22, Handelman discloses: Computing apparatus comprising:

One or more memories adapted to store the instructions of a secure process and an authentication process (col. 5, lines 52-67; col. 7, lines 47-60; col. 9, lines 12-21; col. 11, lines 5-46);

one or more processors arranged to control the operation of the computing apparatus including by executing the secure process and the authentication process (col. 5, lines 52-67; col. 7, lines 47-60; col. 9, lines 12-21; col. 11, lines 5-46);

a user interface arranged to receive user input and return to the user information generated by the one or more processors in response to the user input (col. 11, lines 5-46); and

a token reader interface for receiving and communicating with a removable token, the token having a token memory storing token data including information for identifying the token and auxiliary token information identifying one or more authorized auxiliary tokens (col. 3, lines 30-48; Fig. 4; Fig. 7; col. 4, line 38-col. 5, line 5; col. 8, lines 10-18; col. 15 col. 8, lines 34-60, where the main card also retains billing information of the restricted programs viewable only by using the parent card that corresponds to the auxiliary card),

wherein the one or more processors are arranged to receive the identity information and the auxiliary token information from a primary token received in the token reader interface (Fig. 3, CPU 62; col. 8, lines 10-18, where the main card also retains billing information of the restricted programs viewable only by using the parent card that corresponds to the auxiliary card), authenticate the primary token using the authentication process and, if the primary token is successfully authenticated, permit a

user to interact with the secure process via the user interface (col. 5, line 65-col. 6, lines 6; col. 7, lines 47-56; col. 14, lines 58-66), and cause the computing platform to suspend interaction between the secure process and the user if authentication is not possible as a result of the removal of the primary token unless the primary token is replaced by an authorized auxiliary token (col. 8, lines 19-60; col. 11, lines 32-46, where the absence of smart card corresponds to the recited the removal of the primary token; col. 12, lines 27-29; Fig. 8, where leaving the program scrambled corresponds to the recited to suspend interaction).

However, Handelman does not expressly disclose that the processing means is arranged to repeatedly authenticate the primary token.

Holtey discloses an access control system using smart cards that re-authenticate the system user (corresponding to the recited repeatedly authenticate the primary token) at an adjustable time interval (col. 6, lines 60-col. 7, lines 8).

Therefore, it would have been obvious to a person of ordinary skill in the art at the time the invention was made to implement a periodic authentication (i.e., repeated authentication) measure as taught in Holtey in the system of Handelman because it would provide a mechanism to enforce security (Holtey, col. 7, lines 5-8).

Regarding claim 29, Handelman discloses: Computing apparatus according to claim 22, wherein the primary token comprises a smart card, and the token reader interface is configured to receive a smart card (col. 8, lines 49-60; col. 2, lines 55-59).

2. Claims 2, 16, 23 and 28 are rejected under 35 U.S.C. 103(a) as being unpatentable over Handelman et al (6,298,441 B1; hereinafter Handelman) in view of Holtey (5,442,704) and further in view of Perlman et al (6,173,400; hereinafter Perlman).

Regarding claims 2, 16, 23 and 28, Handelman in view of Holtey discloses that the primary token comprises a token processor (col. 14, lines 25-28). Handelman in view of Holtey does not expressly disclose a computing apparatus according to claim 1, arranged to generate information representing the integrity of the computing apparatus and transmit the integrity information to the primary token (via the trusted device, i.e., card reader), wherein the token processor is programmed to verify the integrity of the computing apparatus including by using the integrity information.

Perlman discloses a method for establishing a shared secret using an authentication token to provide adequate mutual authentication and integrity protection (col. 4, lines 32-43). Perlman further discloses that a smart card can operate as an authentication token to establish a shared secret (corresponding to the recited integrity information) with a remote device to be used for mutual authentication and to check the integrity of the information being transmitted between the smart card and the remote device (corresponding to the verification of the integrity of the remote device or the smart card) (col. 12, lines 1-54).

Therefore, it would have been obvious to a person of ordinary skill in the art at the time the invention was made to implement the use of a share secret between a smart card and a remote device as taught in Perlman in the system of Handelman in

view of Holtey for mutual authentication and integrity check, because it would enhance session security (Perlman, col. 3, lines 1-5).

3. Claim 10, 11, 26 and 27 are rejected under 35 U.S.C. 103(a) as being unpatentable over Handelman et al (6,298,441 B1; hereinafter Handelman) in view of Holtey (5,442,704) and further in view of Lee (5,923,759; hereinafter Lee).

Regarding claim 10, 11, 26 and 27, Handelman in view of Holtey discloses: computing apparatus according to claim 1, wherein the processing means (Fig. 7, CATV Decoder 250) comprises a main processing unit (Fig. 7, CPU 262) and the memory means comprises main memory (Fig. 7, Memory 270).

However, Handelman in view of Holtey does not expressly disclose that the processing means is arranged to comprise a secure processing unit and the memory means comprise a secure memory.

Lee discloses a system for securely exchanging data with smart cards (Fig. 1) that comprises a secure processor (Fig. 1, 122) and a secure data memory (Fig. 1, 126).

Therefore, it would have been obvious to a person of ordinary skill in the art at the time the invention was made to include a secure processor and secure memory area as taught in Lee in the system of Handelman in view of Holtey because it would provide for secure process of encrypting and decrypting data and for secure storage of the encryption keys (Lee, col. 2, lines 50-65).

4. Claim 12 is rejected under 35 U.S.C. 103(a) as being unpatentable over Handelman et al (6,298,441 B1; hereinafter Handelman) in view of Holtey (5,442,704) and further in view of Perlman et al (6,173,400; hereinafter Perlman).

Regarding claim 12, Handelman in view of Holtey discloses that the primary token comprises a token processor (col. 14, lines 25-28). Handelman in view of Holtey does not expressly disclose a computing apparatus according to claim 1, arranged to generate information representing the integrity of the computing apparatus and transmit the integrity information to the primary token, wherein the token processor is programmed to verify the integrity of the computing apparatus including by using the integrity information.

Perlman discloses a method for establishing a shared secret using an authentication token to provide adequate mutual authentication and integrity protection (col. 4, lines 32-43). Perlman further discloses that a smart card can operate as an authentication token to establish a shared secret (corresponding to the recited integrity information) with a remote device to be used for mutual authentication and to check the integrity of the information being transmitted between the smart card and the remote device (corresponding to the verification of the integrity of the remote device or the smart card) (col. 12, lines 1-54).

Therefore, it would have been obvious to a person of ordinary skill in the art at the time the invention was made to implement the use of a share secret between a smart card and a remote device as taught in Perlman in the system of Handelman in

view of Holtey for mutual authentication and integrity check, because it would enhance session security (Perlman, col. 3, lines 1-5).

Allowable Subject Matter

Claims 6, 7, 24 and 25 are objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

Conclusion

The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

US Patent No. 6,405,369 B1 to Tsuria

US Patent No. 5,917,168 to Nakamura et al.

US Patent No. 6,212,635 B1 Reardon

US Patent No. 5,778,072 to Samar

US Patent No. 5,768,382 to Schneier et al.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Abdulhakim Nobahar whose telephone number is 571-272-3808. The examiner can normally be reached on M-T 8-6.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on 571-272-3799. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Abdulhakim Nobahar
Examiner
Art Unit 2132

AN A. N.

February 16, 2005

Gilberto Barron Jr.

GILBERTO BARRÓN JR.
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100